REMARKS

The Office Action dated December 8, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-2, 4-9, 11-16, and 18-25 are currently pending in the application, of which claims 1, 8, 15, 19 and 23-25 are independent claims. Claims 10 and 17 have been cancelled without prejudice or disclaimer. Claim 11 has been amended to more particularly point out and distinctly claim the invention. No new matter has been added. Claims 1-2, 4-9, 11-16, and 18-25 are respectfully submitted for consideration.

The Examiner objected to claims 10 and 17 under 37 C.F.R. 1.75(c) as being improper dependent claims for failing to further limit the subject matter of their respective base claims. Claims 10 and 17 have been cancelled without prejudice or disclaimer. Withdrawal of the objection to claims 10 and 17 is respectfully requested.

Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. The Examiner alleged that the specification "could include signals," and, thus, the claimed subject matter is non-statutory. Applicant respectfully traverses this rejection.

Specifically, Applicant respectfully references page 5, lines 15-20, page 6, lines 9-15 and FIG. 1 of the present application. FIG. 1 illustrates an example system 100 that includes a LAN/WAN and at least one computer device or computer readable medium. A computer readable medium (media and medium may be referred to interchangeably) may be regarded as an electronic device, such as, a personal computer (PC) or multiprocessor system (see page 6, lines 10-12 of the specification).

Applicant notes that §101 governs statutory subject matter. That is, §101 dictates what is considered patentable subject matter and what is not considered patentable subject matter. Regarding what is defined by Applicant's disclosure, §101 is not applicable to defining subject matter, since §101 relates to the claims, not the disclosure. Furthermore, a computer readable medium is recognized as patentable subject matter under §101 and U.S. patent practice. Support for the definition of a computer readable medium is provided by *In re Lowry*, 32 F.3d 1579, 1583-1854, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994), which states: "When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" (see §2106.01 of the MPEP).

Regardless of what is considered patentable subject matter, the specification provides support for a computer readable medium. In addition, claim 25 recites "receiving a request from a client device for access ... to ... a network device." The two **devices** (as devices) recited in claim 25 cannot be limited to mere signals. Therefore, the subject matter recited in claim 25 is statutory under §101 and is supported by the specification as filed. Withdrawal of the rejection is respectfully requested.

Claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* ("Araujo"). Applicant respectfully traverses this rejection.

Claim 1, upon which claims 2 and 4-7 depend, is directed to a method including receiving a request from a client device for access to an application associated with a network device. The method also includes establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device. The method further includes modifying the request at the unified session manager. The method additionally includes forwarding, by the unified session manager, the modified request to the management server. The method also includes receiving a response at the unified session manager from the management server. The method further includes modifying the response at the unified session manager. The method additionally includes forwarding, by the unified session manager, the modified response to the client device.

Claim 8, upon which claims 9 and 11-14 depend, is directed to an apparatus including a transceiver configured to receive a request from a client for access to an application on the network device and to forward a response to the request. The apparatus also includes a processor, coupled to the transceiver. The processor is configured to establish a session on behalf of the client between the unified session manager and a management server associated with the application, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device. The processor is also configured to modify the request. The processor is further configured to forward the modified request to the management server. The processor is additionally configured to receive the response on behalf of the client from the management server associated with the application. The processor is also configured to modify the response. The processor is further configured to forward the modified response from the management server to the transceiver.

Claim 15, upon which claims 16 and 18 depend, is directed to a method including establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients. The method also includes modifying each message from the at least one of the plurality of clients destined for an application associated with the at least one of the plurality of the managements servers, wherein the modification is virtually transparent to the client and to the management server.

Claim 19, upon which claims 20-22 depend, is directed to a method including retrieving a set of menu entries including at least one menu entry that is associated with a remote application. The method also includes displaying a selection menu on a display comprising the set of menu entries. The method further includes retrieving a menu entry selection signal, wherein the menu entry selection signal is modified by a unified session manager. The method additionally includes forwarding the modifying menu entry selection signal to a management server associated with the remote application. The method also includes receiving another signal indicative of a response from the management server, wherein the other signal is modified by the unified session manager. The method further includes establishing a session between the unified session manager and the management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device. The method additionally includes displaying the other modified signal at the display.

Claim 23 is directed to an apparatus including a means for establishing a session with a management server associated with an application on behalf of a remote client, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client. The apparatus also includes a means of modifying a request. The apparatus further includes a first forwarding component configured to forward the modified request to the management server. The apparatus additionally includes a means for receiving a response from the management server. The apparatus also includes a means for modifying the response. The apparatus further includes a second forwarding component configured to forward the modified response to the remote client.

Claim 24 is directed to an apparatus including an establisher configured to establish a session with a management server associated with an application on behalf of a remote client, wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client. The apparatus also includes a modifier configured to modify a request. The apparatus further includes a request forwarder configured to forward the modified request to the management server. The apparatus additionally includes a receiver configured to receive a response from the management server. The apparatus also includes a modifier configured to modify the response. The apparatus further includes a response forwarder configured to forward the modified response to the remote client.

Claim 25 is directed to a computer program embodied on a computer readable medium. The computer program is configured to control a processor to perform receiving a request from a client device for access to an application associated with a network device. The computer program is also configured to control a processor to perform establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device. The computer program is further configured to control a processor to perform modifying the request at the unified session manager. The computer program is additionally configured to control a processor to perform forwarding, by the unified session manager, the modified request to the management server. The computer program is also configured to control a processor to perform receiving a response at the unified session manager from the management server. The computer program is further configured to control a processor to perform modifying the response at the unified session manager. The computer program is additionally configured to control a processor to perform forwarding, by the unified session manager, the modified response to the client device.

Applicant respectfully submits that Araujo fails to disclose, suggest, or otherwise render obvious all of the features of any of the presently pending claims.

Araujo generally relates to an apparatus and accompanying methods for providing, through a centralized server site, an integrated virtual office environment, remotely accessible via a network-connected web browser, with remote network monitoring and management capabilities. In Araujo, a front end (a service enablement platform (SEP)) to one or more office servers on a LAN is connected to both the WAN and LAN and acts as a bridge between the user and the user's office applications. The front end also acts as a protocol translator to enable bi-directional, web-based, real-time communication to occur between the browser and each such application.

The Office Action has recognized that Araujo does not explicitly disclose that the feature of establishing a session between a unified session manager (SEP 200 of Araujo in the Office Action's view) and a management server associated with an application comprises authenticating the unified session manager to the management server. However, the Office Action appears to have considered that this is implicit in Araujo, referring to paragraph [0109] of Araujo, which discloses that all information transfer for the Netilla virtual office is protected by SSL.

As such, the Office Action considered that the SEP and the application servers of Araujo communicate using SSL and that using SSL is known to inherently include an authentication step. Accordingly, the Office Action concluded that the SEP and the application servers authenticate themselves utilizing the SSL protocol in Araujo.

The Office Action's analysis is incorrect. While the Office Action is correct that the SSL protocol can include an authentication step, the Office Action is incorrect that the SEP and the application servers communicate using SSL in Araujo. Although Araujo does state in paragraph [0109] that for the Netilla virtual office, all information transfer is protected by SSL, if one reads further from this disclosure, it is made clear by Araujo that SSL encryption and decryption is only utilized for all communications **to and from the remote client via the WAN** and is not in fact used for communications **between the SEP and the LAN** including the application servers.

In paragraph [0109] of Araujo, it is explained that when an incoming packet is received at the SEP from the client device via the WAN connection, the open SSL module 304 performs SSL processing on the packet. This may implicitly involve authenticating the packet as suggested by the Office Action. It is then stated that after SSL processing, the HTTP request is extracted and sent to the virtual office software 400 for translation into a form suitable for use by a desired office application. Once virtual office software 400 has properly processed the information, by providing suitable protocol conversion, that information flows **directly** from software 400 to the office application. Thus, it is clear that the incoming packet is authenticated and decrypted prior to extraction of the content of the packet extraction and subsequent translation by the virtual office software 400. The HTTP request is thus extracted, translated and sent directed to the office application without passing back via the open SSL module 340 for encryption prior to being sent to the application server. As such, there is no SSL encryption used for communications between the SEP and the application server.

The aforementioned interpretation (*i.e.* Applicant's interpretation) is confirmed as being correct with further reference to the disclosure in paragraph [0111] of Araujo, which describes the processing of packets received by the SEP from the LAN. These packets are received along data path 402 shown in Figure 3b. This path flows through to the virtual office software 400 without passing through web server 350 and without calling on the open SSL module 340. The virtual office software 400 generates an appropriate HTML page and only then passes the HTML page to web server 350. The web server 350 then calls on the services of the open SSL module 340 to encrypt the HTML page and send it to the remote client via the WAN.

In light of the above, it is clear that the mention of "all information transfer is protected by SSL" in paragraph [0109] of Araujo actually relates to all information transferred **between the remote client and the SEP via the WAN**. No authentication and encryption protocols are utilized between the SEP and the LAN.

If there is any further doubt regarding the aforementioned analysis, Applicant respectfully further points out that the reason no encryption protocol is required in Araujo between the SEP and the LAN is that the SEP is authenticated during an initial installation process with the centralized administrative website (referred to as "customer care centre" (CCC)). This is described, for example, in paragraphs [0038] to [0041] of Araujo.

In light of the above, it is clear that there is no disclosure or suggestion in Araujo that establishing a session between the SEP and management server associated with an application comprises authenticating the SEP with the management server associated with the application. Rather, the SEP in Araujo is authenticated with a centralized administrative website (CCC) during installation and subsequent communications between a remote client and the SEP via the WAN are encrypted and decrypted using SSL.

The arrangement described in Araujo is adapted for use in small to medium sized organizations and specifically for remotely accessing an internal office network remotely by employees. A centralized administrative website (CCC) is used for remote network monitoring and management functionality. No authentication or encryption protocols are required between the SEP and the LAN as these are all located within the local office network environment. In contrast, certain embodiments of the present invention are directed to a method and system for managing multiple management servers via a single unified session manager to provide a unified session control for general services over the internet to internet users who may not necessarily be employees looking to remotely access a local office network. As such, the applications and management servers associated therewith may not be provided in a safe office intranet environment. Accordingly, the arrangement of Araujo is not appropriate for the use intended for the present invention. For more general internet usage, it has been found by the present inventors to be advantageous that when a request is received from a client device for accessing an application, the step of establishing a session between a unified session manager and a management server associated with the application comprises authenticating the unified session manager to the management server. Such an authentication process is not required in Araujo.

Accordingly, it has been demonstrated that Araujo fails to disclose or suggest at least "wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device" (as recited in claim 1), or the similar recitations found in independent claims 8, 15, 19, and 23-25, each of which has its own respective scope. It is, therefore, respectfully requested that the rejection of claims 1, 8, 15, 19, and 23-25 be withdrawn.

Claims 2, 4-7, 9, 11-14, 16, 18, and 20-22 depend respectively from, and further limit, claims 1, 8, 15, and 19. Thus, each of claims 2, 4-7, 9, 11-14, 16, 18, and 20-22 recites subject matter that is neither disclosed nor suggested by Araujo. Claims 10 and 17 have been cancelled without prejudice or disclaimer. It is, therefore, respectfully requested that the rejection of claims 2, 4-7, 9-14, 16-18, and 20-22 be withdrawn.

For the reasons set forth above, it is respectfully submitted that each of claims 1-2, 4-9, 11-16, and 18-25 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-2, 4-9, 11-16, and 18-25 be allowed, and that this application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Peter Flanagan

Peter Flanagan
Attorney for Applicant
Registration No. 58,178

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

PCF/dlh